Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO

zwischen

[Name und Adresse des Auftraggebers]

– nachfolgend „Auftraggeber“ –

und

Eniyan GmbH, Hasenhügel 4, 48485 Neuenkirchen

– nachfolgend „Auftragnehmer“ –

1. Gegenstand und Dauer der Verarbeitung

(1) Gegenstand:

Gegenstand dieses Vertrags ist die Verarbeitung personenbezogener Daten im Rahmen der zwischen den Parteien bestehenden Dienstleistungsvereinbarung (z. B. Social Media Management, Content-Erstellung, Support).

(2) Dauer:

Die Laufzeit dieses Vertrags entspricht der Laufzeit der Dienstleistungsvereinbarung. Die Verpflichtungen aus diesem Vertrag gelten, solange der Auftragnehmer personenbezogene Daten des Auftraggebers verarbeitet.

2. Art und Zweck der Verarbeitung, Kategorien personenbezogener Daten, betroffene Personen

(1) Art und Zweck der Verarbeitung:

Die Verarbeitung erfolgt ausschließlich zur Erfüllung der vertraglich vereinbarten Dienstleistungen.

(2) Kategorien personenbezogener Daten:

- Log-in-Daten
- Vertragsstammdaten
- Kundenhistorie
- Beschäftigtendaten

- IBANs (verschlüsselt)
- Weitere Daten gemäß Leistungsbeschreibung

(3) Kategorien betroffener Personen:

- Kunden
- Interessenten
- Beschäftigte des Auftraggebers

3. Rechte und Pflichten des Auftraggebers

- Der Auftraggeber ist für die Rechtmäßigkeit der Datenverarbeitung verantwortlich.
- Er ist berechtigt, Weisungen zu erteilen und die Einhaltung der Vereinbarung zu kontrollieren.
- Änderungen des Verarbeitungsgegenstands und der Verfahren erfolgen nur auf Weisung des Auftraggebers.

4. Pflichten des Auftragnehmers

- Verarbeitung ausschließlich auf dokumentierte Weisung des Auftraggebers.
- Verpflichtung zur Vertraulichkeit aller mit der Verarbeitung befassten Personen.
- Umsetzung und Nachweis der in Anlage 1 beschriebenen technischen und organisatorischen Maßnahmen (TOM).
- Unterstützung bei Betroffenenrechten und Meldepflichten.
- Unterstützung bei Datenschutz-Folgenabschätzungen.
- Information bei behördlichen Maßnahmen oder Datenschutzvorfällen.
- Löschung oder Rückgabe aller personenbezogenen Daten nach Vertragsende.

5. Technisch-organisatorische Maßnahmen (TOM)

Die TOM gemäß Art. 32 DSGVO sind in Anlage 1 beschrieben und Bestandteil dieses Vertrags. Der Auftragnehmer stellt sicher, dass das Schutzniveau stets angemessen ist und informiert den Auftraggeber über wesentliche Änderungen.

6. Unterauftragsverhältnisse

- Der Einsatz von Unterauftragnehmern/Subunternehmern ist zulässig, sofern sie die Anforderungen dieses Vertrags und der DSGVO erfüllen.

- Die folgenden Unterauftragnehmer werden aktuell eingesetzt:
    - Microsoft Ireland Operations Ltd. (Microsoft Dynamics, Microsoft 365; Datenverarbeitung ggf. auch in den USA, Schutz gemäß Standardvertragsklauseln und Zusatzmaßnahmen von Microsoft Deutschland)
    - Haufe-Lexware GmbH & Co. KG (LexOffice) – Datenverarbeitung in Deutschland
    - rapidmail GmbH (E-Mail-Marketing, Serverstandort Deutschland)
    - Automattic Inc. / WooCommerce (Shop-System, Datenverarbeitung in der EU oder nach Hosting-Standort; Standardvertragsklauseln bei Drittlandübermittlung)
    - Superchat GmbH (Kommunikationsplattform, Serverstandort Deutschland/EU)
- Weitere Unterauftragnehmer dürfen nur nach vorheriger Information und Zustimmung des Auftraggebers eingesetzt werden.

7. Internationale Datenübermittlung

- Eine Übermittlung personenbezogener Daten in Drittländer (insbesondere USA) erfolgt nur, soweit dies zur Vertragserfüllung erforderlich ist und unter Einhaltung der gesetzlichen Vorgaben (insbesondere Standardvertragsklauseln der EU-Kommission und ergänzende Schutzmaßnahmen von Microsoft bzw. Automattic/WooCommerce).
- Der Auftragnehmer informiert den Auftraggeber über geplante internationale Übermittlungen.

8. Kontrollrechte und Mitwirkungspflichten

- Der Auftraggeber ist berechtigt, die Einhaltung der Vereinbarung zu kontrollieren.
- Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung seiner Pflichten.

9. Weisungsbefugnis

- Der Auftragnehmer verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Auftraggebers.
- Bei rechtswidrigen Weisungen informiert der Auftragnehmer den Auftraggeber unverzüglich.

10. Löschung und Rückgabe von Daten

- Nach Abschluss der vertraglichen Leistungen oder auf Weisung des Auftraggebers werden alle personenbezogenen Daten gelöscht oder zurückgegeben, sofern keine gesetzlichen Aufbewahrungspflichten entgegenstehen.
- Die Löschung ist zu dokumentieren und auf Verlangen nachzuweisen.

11. Elektronische Signatur

- Dieser Vertrag kann auch elektronisch unterzeichnet werden; eine handschriftliche Unterschrift ist nicht erforderlich.

Im Falle von Widersprüchen zwischen dem Hauptvertrag und dieser Vereinbarung gelten die Regelungen dieser Auftragsverarbeitung vorrangig, soweit es Datenschutzbelange betrifft.

12. Schlussbestimmungen

- Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform (auch elektronisch möglich).
- Sollte eine Bestimmung dieses Vertrags unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

Ort, Datum

_____ (Auftraggeber)

_____ (Auftragnehmer)

Anlage 1: Technisch-organisatorische Maßnahmen (TOM)

1. Vertraulichkeit
- Zutrittskontrolle: Remote-Arbeiten, gesicherte Zugänge, ggf. Büroabsicherung
- Zugangskontrolle: Benutzername/Passwort, Zwei-Faktor-Authentifizierung, zentrale Passwortvergabe
- Zugriffskontrolle: Berechtigungskonzepte, Protokollierung, minimale Anzahl an Administratoren
- Trennungskontrolle: Mandantentrennung, getrennte Datenhaltung, Verarbeitung nur in Kundensystemen
- Pseudonymisierung/Anonymisierung, wo möglich

2. Integrität
- Weitergabekontrolle: Verschlüsselung bei Übertragung (z. B. https), Protokollierung von Zugriffen
- Eingabekontrolle: Protokollierung von Änderungen, individuelle Nutzerkennung

3. Verfügbarkeit und Belastbarkeit
- Regelmäßige Backups
- Notfallmanagement, Wiederherstellungspläne
- Schutz vor Viren und Malware (Firewall, Antivirensoftware)

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung
- Datenschutzbeauftragter (intern/extern)
- Schulung der Mitarbeitenden
- Regelmäßige Überprüfung der TOM
- Incident-Response-Management

5. Weitere Maßnahmen
- Dokumentation der Prozesse
- Auftragskontrolle bei Unterauftragnehmern
- Keine Verarbeitung besonderer Kategorien personenbezogener Daten

Hinweis: Diese TOM sind regelmäßig zu überprüfen und an den Stand der Technik anzupassen.